Abstract

A technique for secure file access control via directory encryption. Filenames of data files stored by a network server are encrypted so as to protect them in the event the server is untrustworthy, such as in a distributed computing environment. Two encryption keys are employed so as to provide different access capabilities. For example, clients of the server that are authorized to perform read-only operations on the files may be prevented from modifying the files, while client that are authorized to perform write operations, may modify the files or even delete the files. In a preferred embodiment, encrypted filenames replace plaintext files in a directory structure without otherwise changing the directory structure. Because the directory structure is otherwise unchanged, the server may still have adequate information to perform file management and space management functions.